UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,402	07/31/2003	Alan H. Karp	200311103-1	2929

22879 7590 04/25/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
WEINTROP, ADAM S	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/632,402	KARP, ALAN H.	
	Examiner	Art Unit	
	Adam S. Weintrop	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/25/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. **Claims 1-39** are objected to because of the following informalities:

Regarding **claims 1-39**, the preamble of all the claims recites "increasing message costs" or "increasing message transaction costs". This purpose of the invention does not convey a useful purpose and should be changed to --increasing message transaction costs to minimize junk or spam emails-- in order to clarify the purpose of the invention.

Regarding **claim 1**, the term "a message" on line 5 has already been defined and should be replaced with --the message--. The term "the recipient address" on line 5-6 has already been defined and should be replaced with --the recipient address--.

Regarding **claim 9**, the term "a request" on line 2 should be replaced with --the request--.

Regarding **claim 10**, the term "the sending computer" on line 4 has not been defined and should be replaced with --a sending computer--.

Regarding **claim 19**, the term "the receiving element" on line 6 has not been defined and should be replaced with --a receiving element--.

Regarding **claim 20**, the claim ends with a ";". The claim needs to end with a --.--

Regarding **claim 25**, the term "the sending computer" on lines 4-5 has not yet been defined and should be replaced with --a sending computer--.

Regarding **claim 34**, the term "a recipient address" on lines 6-7 has already been defined and should be replaced with --the recipient address.

Regarding **claim 35**, the term "the sending computer" on line 5 has not yet been defined and should be replaced with --a sending computer--.

Regarding **claim 36**, the term "the receiving element" on line 6 has not been defined and should be replaced with --a receiving element--.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1, 8-9, and 34** are rejected under 35 U.S.C. 102(e) as being anticipated by Petry et al. (US 6,941,348).

Regarding **claim 1**, Petry et al. anticipates a method for increasing message costs, comprising: receiving over a data link a request to route a message to a recipient address (column 6, lines 36-41, with the system receiving and delivering through the EMS server, which intercepts the request to route an email); calculating a delay period,

in response to the request (column 13, lines 22-48, with the expiration time being calculated, or made into use, in response to the connection request, and the expiration time delays mail servers); dropping the data link (column 13, lines 42-48, with the connection manager blocking connections if the expiration time is not yet reached, seen as dropping the connection link); receiving over the data link a next request to route a message to a recipient address (column 10, lines 10-19, with subsequent request being handled by the disposition flags); dropping the data link, if the next request was received during the delay period (column 9, lines 53-62, with the disposition flags being configured based on the expiration time, and these flags can be a message reject, seen as dropping the connection link); and routing the message referenced in the next request to the recipient address, if the delay period has expired (column 13, lines 46-52, with the connection manger processing the messages once the expiration time has expired).

Regarding **claim 8**, Petry et al. anticipates the method of claim 1, wherein the message is an email message (Abstract).

Regarding **claim 9**, Petry et al. anticipates the method of claim 1, wherein the receiving element includes receiving over the data link a request to route the message from a particular sending computer to the recipient address hosted by a particular receiving computer (column 5, lines 1-12 and 52-64, with an explanation of email message sending requests).

Regarding **claim 34**, Petry et al. anticipates a system for increasing message transaction costs, comprising a: means for receiving over a data link a request to route

a message to a recipient address (column 6, lines 36-41, with the system receiving and delivering through the EMS server, which intercepts the request to route an email); means for calculating a delay period, in response to the request (column 13, lines 22-48, with the expiration time being calculated, or made into use, in response to the connection request, and the expiration time delays mail servers); means for dropping the data link (column 13, lines 42-48, with the connection manager blocking connections if the expiration time is not yet reached, seen as dropping the connection link); means for receiving over the data link a next request to route a message to a recipient address (column 10, lines 10-19, with subsequent request being handled by the disposition flags); means for dropping the data link, if the next request was received during the delay period (column 9, lines 53-62, with the disposition flags being configured based on the expiration time, and these flags can be a message reject, seen as dropping the connection link); and means for routing the message referenced in the next request to the recipient address, if the delay period has expired (column 13, lines 46-52, with the connection manger processing the messages once the expiration time has expired).

4. **Claims 10-12, 17-18, and 35** are rejected under 35 U.S.C. 102(e) as being anticipated by Drummond et al. (US 6,691,156).

Regarding **claim 10**, Drummond et al. anticipates a method for increasing message transaction costs, comprising: receiving over a data link a request to route a message to a recipient address (column 6, lines 27-29, where a return email generated, seen as requesting a message to route to a recipient address); attempting to identify the recipient address (column 6, lines 35-40, with the new recipient address being identified

before the original message is delivered); and dropping the data link with the sending computer, if the recipient address can not be identified (column 6, lines 40-49, with the message being erased if the address can not be identified, seen as dropping the communication link).

Regarding **claim 11**, Drummond et al. anticipates the method of claim 10, wherein the attempting element includes attempting to verify that the recipient address is valid (column 6, lines 35-40, with the identifying process seeking validation of the email address).

Regarding **claim 12**, Drummond et al. anticipates the method of claim 10, wherein the attempting element includes attempting to verify that the recipient address known (column 6, lines 35-53, with the identifying process seeking validation of the email address, and this validation is made by a response from the email address, equivalent to seeking if the address is known).

Regarding **claims 17-18**, Drummond et al. anticipates the method of claim 10, wherein the message is an email message and the address is an email address (column 2, lines 23-36, with the system being used for email messages in accordance with email addresses).

Regarding **claim 35**, Drummond et al. anticipates a system for increasing message transaction costs, comprising a: means for receiving over a data link a request to route a message to a recipient address (column 6, lines 27-29, where a return email generated, seen as requesting a message to route to a recipient address); means for attempting to identify the recipient address (column 6, lines 35-40, with the new

recipient address being identified before the original message is delivered); and means for dropping the data link with the sending computer, if the recipient address can not be identified (column 6, lines 40-49, with the message being erased if the address can not be identified, seen as dropping the communication link).

5. **Claims 19-20, 25-26, 29, 31-33, and 36-38** are rejected under 35 U.S.C. 102(e) as being anticipated by MacIntosh et al. (US 6,973,481).

Regarding **claim 19**, MacIntosh et al. anticipates a method for increasing message transaction costs, comprising: generating a first set of faux addresses (column 8, lines 42-45, with faux addresses seen as fake or alias addresses); making the faux addresses available (column 9, lines 16-56, with the alias email being made available to the website requesting the address); receiving over a data link a request to route a message to a faux address within the set of faux addresses (column 12, lines 18-23, with the email client getting email at the alias address); and dropping the data link, in response to the receiving element (column 12, lines 24-54, with the email message being deleted in response to the client's alias settings, seen as dropping the communication link).

Regarding **claim 20**, MacIntosh et al. anticipates the method of claim 19: wherein the making element includes, publishing the faux addresses on a public network (column 9, lines 16-56, with the alias email being made available to the website requesting the address, a website being part of the Internet, a public network).

Regarding **claim 25**, MacIntosh et al. anticipates the method of claim 19: further comprising, treating the faux address as valid for a predetermined period of time, in

response to the receiving element (column 11, lines 23-30, where the alias email is valid for a predetermined time as set by the client); and wherein the dropping element includes, dropping the data link with the sending computer, after the predetermined period of time has expired (column 11, lines 23-30, with an expiration value disabling the alias email and column 12, lines 35-44, with the message being deleted in response to a disabled alias address, seen as dropping the communication path).

Regarding **claim 26**, MacIntosh et al. anticipates the method of claim 25: wherein the treating element includes providing a faux validation of the faux address back over the data link (column 12, lines 18-24, with the alias address being validated by checking its enabled status, and this information is sent back to the mail servers to inform the alias' validation status).

Regarding **claim 29**, MacIntosh et al. anticipates the method of claim 19: further comprising, treating the faux address as valid until a number of messages addressed to the faux address reaches a first predetermined number within a first predetermined time period (column 11, lines 23-30, with the expiration of an alias criteria being functions of time and amount used); and wherein the dropping element includes, dropping the data link, after the number of messages addressed to the faux address exceeds the first predetermined number within the first predetermined time period (column 11, lines 23-30, with an expiration value disabling the alias email and column 12, lines 35-44, with the message being deleted in response to a disabled alias address, seen as dropping the communication path).

Regarding **claim 31**, MacIntosh et al. anticipates the method of claim 19, further comprising: generating a next set of faux addresses; repeating the making, receiving, and dropping elements with respect to the next set of faux addresses (column 10, lines 28-59, with the user being able to generate more than one faux addresses and make them available on the Internet, column 12, lines 18-23, with the email client getting email at any alias address, and column 12, lines 24-54, with the email message being deleted in response to the client's alias settings, seen as dropping the communication link).

Regarding **claims 32 and 33**, MacIntosh et al. anticipates the method of claim 19, wherein the message is an e-mail message and the address is an e-mail address (Abstract).

Regarding **claim 36**, MacIntosh et al. anticipates a system for increasing message transaction costs, comprising a: means for generating a first set of faux addresses (column 8, lines 42-45, with faux addresses seen as fake or alias addresses); means for making the faux addresses available (column 9, lines 16-56, with the alias email being made available to the website requesting the address); means for receiving over a data link a request to route a message to a faux address within the set of faux addresses (column 12, lines 18-23, with the email client getting email at the alias address); and means for dropping the data link, in response to the receiving element (column 12, lines 24-54, with the email message being deleted in response to the client's alias settings, seen as dropping the communication link).

Regarding **claim 37**, MacIntosh et al. anticipates the system of claim 36, further comprising: means for treating the faux address as valid for a predetermined period of time, in response to the receiving element (column 11, lines 23-30, where the alias email is valid for a predetermined time as set by the client).

Regarding **claim 38**, MacIntosh et al. anticipates the system of claim 36, further comprising: means for treating the faux address as valid until a number of messages addressed to the faux address reaches a first predetermined number within a first predetermined time period (column 11, lines 23-30, with the expiration of an alias criteria being functions of time and amount used).

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. **Claims 19-20, 31-33, and 36** are rejected under 35 U.S.C. 102(b) as being anticipated by Levosky (US 2002/0087641).

Regarding **claim 19**, Levosky anticipates a method for increasing message transaction costs, comprising: generating a first set of faux addresses (section 0038 and 0048, with alias emails being generated); making the faux addresses available (section 0048, with the address being made available by using it on the Internet, or in any communication); receiving over a data link a request to route a message to a faux address within the set of faux addresses (section 0049, with the alias email address receiving a email message); and dropping the data link, in response to the receiving

element (sections 0063 and 0065, with the user being able to block and suspend communication directed towards the alias addresses, seen as dropping the communication path).

Regarding **claim 20**, Levosky anticipates the method of claim 19: wherein the making element includes, publishing the faux addresses on a public network (section 0048, with the address being made available by using it on the Internet, seen as a public network, or in any communication).

Regarding **claim 31**, Levosky anticipates the method of claim 19, further comprising: generating a next set of faux addresses; repeating the making, receiving, and dropping elements with respect to the next set of faux addresses (section 0047, with the user being able to create multiple alias emails, and section 0048, with the address being made available by using it on the Internet, or in any communication, section 0049, with the alias email address receiving a email message, and sections 0063 and 0065, with the user being able to block and suspend communication directed towards the alias addresses, seen as dropping the communication path).

Regarding **claims 32 and 33**, Levosky anticipates the method of claim 19, wherein the message is an e-mail message and the address is an e-mail address (Abstract).

Regarding **claim 36**, Levosky anticipates a system for increasing message transaction costs, comprising a: means for generating a first set of faux addresses (section 0038 and 0048, with alias emails being generated); means for making the faux addresses available (section 0048, with the address being made available by using it on

the Internet, or in any communication); means for receiving over a data link a request to route a message to a faux address within the set of faux addresses (section 0049, with the alias email address receiving a email message); and means for dropping the data link, in response to the receiving element (sections 0063 and 0065, with the user being able to block and suspend communication directed towards the alias addresses, seen as dropping the communication path).

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

9. **Claims 1, 3, 8-9, and 34** are rejected under 35 U.S.C. 102(a) as being anticipated by "The Next Step in the Spam Control War: Greylisting" (Harris).

Regarding **claim 1**, Harris anticipates a method for increasing message costs, comprising: receiving over a data link a request to route a message to a recipient address (page 4, lines 25-41, with the greylisting process passing or denying mail, which inherently includes receiving requests for mail to be sent to a recipient address); calculating a delay period, in response to the request (page 4, lines 25-41, with the email triplet being responded to by the block placed on it, these blocks are calculated by configuration parameters seen in page 6, lines 15-32); dropping the data link (page 4, lines 25-41, with the communication path failing if the mail has not been seen yet); receiving over the data link a next request to route a message to a recipient address (page 4, lines 25-41, with receiving a subsequent request); dropping the data link, if the

next request was received during the delay period (page 4, lines 25-41, with the request being blocked if the corresponding block is not expired); and routing the message referenced in the next request to the recipient address, if the delay period has expired (page 4, lines 25-41, with the email passing if the block has expired).

Regarding **claim 3**, Harris anticipates the method of claim 1, wherein the calculating element includes calculating a random delay period (page 6, lines 12-14, with the delay period being able to vary from installation to installation).

Regarding **claim 8**, Harris anticipates the method of claim 1, wherein the message is an email message (page 4, lines 25-41, with the implementation made for email messages).

Regarding **claim 9**, Harris anticipates the method of claim 1, wherein the receiving element includes receiving over the data link a request to route the message from a particular sending computer to the recipient address hosted by a particular receiving computer (page 2, lines 17-24, with the triplet being made of sending address and receiving address).

Regarding **claim 34**, Harris anticipates a system for increasing message transaction costs, comprising a: means for receiving over a data link a request to route a message to a recipient address (page 4, lines 25-41, with the greylisting process passing or denying mail, which inherently includes receiving requests for mail to be sent to a recipient address); means for calculating a delay period, in response to the request (page 4, lines 25-41, with the email triplet being responded to by the block placed on it, these blocks are calculated by configuration parameters seen in page 6, lines 15-32);

means for dropping the data link (page 4, lines 25-41, with the communication path failing if the mail has not been seen yet); means for receiving over the data link a next request to route a message to a recipient address (page 4, lines 25-41, with receiving a subsequent request); means for dropping the data link, if the next request was received during the delay period (page 4, lines 25-41, with the request being blocked if the corresponding block is not expired); and means for routing the message referenced in the next request to the recipient address, if the delay period has expired (page 4, lines 25-41, with the email passing if the block has expired).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Petry et al. (US 6,941,348) on view of McDowell et al. (US 2002/0035605).

Regarding **claim 2**, Petry et al. discloses all of the limitations as described above except for calculating the delay period once per day. Petry et al. teaches that the records for calculating delay are updated through an administrative console or in other databases. The general concept of updating a calculation based in a configuration system once a day is well known in the art as illustrated by McDowell et al. McDowell et al. teaches a presence location system in which a user can filter out subscription

services according to their preferences (section 0171), and this system can be updated daily in order to change their preferences regarding what subscriber can receive the user's presence information, seen as modifying a parameter for unsolicited services daily (sections 0130-0131). It would have been obvious to one of ordinary skill in the art at the time of invention to modify Petry et al. with updating parameters daily as taught by McDowell et al. in order to create a more permission-oriented system as to increase the control the user has over the system.

12. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over "The Next Step in the Spam Control War: Greylisting" (Harris) in view of McDowell et al. (US 2002/0035605).

Regarding **claim 2**, Harris discloses all of the limitations as described above except for calculating the delay period once per day. Harris teaches that the records for calculating delay are set at installation time (page 6, lines 4-17). The general concept of updating a calculation based in a configuration system once a day is well known in the art as illustrated by McDowell et al. McDowell et al. teaches a presence location system in which a user can filter out subscription services according to their preferences (section 0171), and this system can be updated daily in order to change their preferences regarding what subscriber can receive the user's presence information, seen as modifying a parameter for unsolicited services daily (sections 0130-0131). It would have been obvious to one of ordinary skill in the art at the time of invention to modify Harris with updating parameters daily as taught by McDowell et al. in order to

create a more permission-oriented system as to increase the control the user has over the system.

13. **Claims 4-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Petry et al. (US 6,941,348) on view of Transmission Control Protocol (TCP Specification).

Regarding **claims 4-5**, Petry et al. discloses all of the limitations as described above except for dropping the link by using a transport layer command, or using the TCP command "FIN" to drop the link. The general concept of dropping a link using the TCP command "FIN", which is a transport layer command is well known in the art as illustrated by TCP. TCP Specification teaches closing connections with the "FIN" command in section 3.5, on page 37. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Petry et al. with using a TCP connection close command as taught by the TCP Specification in order to reliably close the connection between the pairs of processes as noted in section 1.1 on page 1.

14. **Claims 4-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over "The Next Step in the Spam Control War: Greylisting" (Harris) in view of Transmission Control Protocol (TCP Specification).

Regarding **claims 4-5**, Harris discloses all of the limitations as described above except for dropping the link by using a transport layer command, or using the TCP command "FIN" to drop the link. The general concept of dropping a link using the TCP command "FIN", which is a transport layer command is well known in the art as illustrated by TCP. TCP Specification teaches closing connections with the "FIN"

command in section 3.5, on page 37. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Harris with using a TCP connection close command as taught by the TCP Specification in order to reliably close the connection between the pairs of processes as noted in section 1.1 on page 1.

15. **Claims 6-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Petry et al. (US 6,941,348) on view of Iptables.

Regarding **claims 6-7**, Petry et al. discloses all of the limitations as described above except for closing a connection using the network layer, or an IP layer, without sending messages back over the data link. In applicant's specification on page 10, lines 13-19, this can be accomplished with modification of a firewall code as to block TCP messages. The general concept of using a firewall to block certain TCP messages is well known in the art as illustrated by Iptables. Iptables is a firewall for computers in which the codes can be simply defined in tables of rules. The options can delete the packets as described in page 2, specify what protocol to watch for as described in page 3, and specify what TCP extensions to watch for in page 5. Using this firewall setup, a server could effectively block outgoing TCP FIN messages, therefore creating, according to the applicant, a silent network layer or IP layer connection drop. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Petry et al. with using firewall codes as taught by Iptables in order to make use of the firewall's features and change them to silently close the connections as to reduce network congestion by eliminating TCP packets.

16. **Claims 6-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over "The Next Step in the Spam Control War: Greylisting" (Harris) in view of Iptables.

Regarding **claims 6-7**, Harris discloses all of the limitations as described above except for closing a connection using the network layer, or an IP layer, without sending messages back over the data link. In applicant's specification on page 10, lines 13-19, this can be accomplished with modification of a firewall code as to block TCP messages. The general concept of using a firewall to block certain TCP messages is well known in the art as illustrated by Iptables. Iptables is a firewall for computers in which the codes can be simply defined in tables of rules. The options can delete the packets as described in page 2, specify what protocol to watch for as described in page 3, and specify what TCP extensions to watch for in page 5. Using this firewall setup, a server could effectively block outgoing TCP FIN messages, therefore creating, according to the applicant, a silent network layer or IP layer connection drop. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Harris with using firewall codes as taught by Iptables in order to make use of the firewall's features and change them to silently close the connections as to reduce network congestion by eliminating TCP packets.

17. **Claims 13-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al. (US 6,691,156) in view of Transmission Control Protocol (TCP Specification).

Regarding **claims 13-14**, Drummond et al. discloses all of the limitations as described above except for dropping the link by using a transport layer command, or

using the TCP command "FIN" to drop the link. The general concept of dropping a link using the TCP command "FIN", which is a transport layer command is well known in the art as illustrated by TCP. TCP Specification teaches closing connections with the "FIN" command in section 3.5, on page 37. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Drummond et al. with using a TCP connection close command as taught by the TCP Specification in order to reliably close the connection between the pairs of processes as noted in section 1.1 on page 1.

18. **Claims 15-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al. (US 6,691,156) in view of Iptables.

Regarding **claims 15-16**, Drummond et al. discloses all of the limitations as described above except for closing a connection using the network layer, or an IP layer, without sending messages back over the data link. In applicant's specification on page 10, lines 13-19, this can be accomplished with modification of a firewall code as to block TCP messages. The general concept of using a firewall to block certain TCP messages is well known in the art as illustrated by Iptables. Iptables is a firewall for computers in which the codes can be simply defined in tables of rules. The options can delete the packets as described in page 2, specify what protocol to watch for as described in page 3, and specify what TCP extensions to watch for in page 5. Using this firewall setup, a server could effectively block outgoing TCP FIN messages, therefore creating, according to the applicant, a silent network layer or IP layer connection drop. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Drummond et al. with using firewall codes as taught by Iptables in order to make use of

the firewall's features and change them to silently close the connections as to reduce network congestion by eliminating TCP packets.

19. **Claims 21-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over MacIntosh et al. (US 6,973,481) in view of Transmission Control Protocol (TCP Specification).

Regarding **claims 21-22**, MacIntosh et al. discloses all of the limitations as described above except for dropping the link by using a transport layer command, or using the TCP command "FIN" to drop the link. The general concept of dropping a link using the TCP command "FIN", which is a transport layer command is well known in the art as illustrated by TCP. TCP Specification teaches closing connections with the "FIN" command in section 3.5, on page 37. It would have been obvious to one of ordinary skill in the art at the time of invention to modify MacIntosh et al. with using a TCP connection close command as taught by the TCP Specification in order to reliably close the connection between the pairs of processes as noted in section 1.1 on page 1.

20. **Claims 21-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Levosky (US 2002/0087641) in view of Transmission Control Protocol (TCP Specification).

Regarding **claims 21-22**, Levosky discloses all of the limitations as described above except for dropping the link by using a transport layer command, or using the TCP command "FIN" to drop the link. The general concept of dropping a link using the TCP command "FIN", which is a transport layer command is well known in the art as illustrated by TCP. TCP Specification teaches closing connections with the "FIN"

command in section 3.5, on page 37. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Levosky with using a TCP connection close command as taught by the TCP Specification in order to reliably close the connection between the pairs of processes as noted in section 1.1 on page 1.

21. **Claims 23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over MacIntosh et al. (US 6,973,481) in view of Iptables.

Regarding **claims 23-24**, MacIntosh et al. discloses all of the limitations as described above except for closing a connection using the network layer, or an IP layer, without sending messages back over the data link. In applicant's specification on page 10, lines 13-19, this can be accomplished with modification of a firewall code as to block TCP messages. The general concept of using a firewall to block certain TCP messages is well known in the art as illustrated by Iptables. Iptables is a firewall for computers in which the codes can be simply defined in tables of rules. The options can delete the packets as described in page 2, specify what protocol to watch for as described in page 3, and specify what TCP extensions to watch for in page 5. Using this firewall setup, a server could effectively block outgoing TCP FIN messages, therefore creating, according to the applicant, a silent network layer or IP layer connection drop. It would have been obvious to one of ordinary skill in the art at the time of invention to modify MacIntosh et al. with using firewall codes as taught by Iptables in order to make use of the firewall's features and change them to silently close the connections as to reduce network congestion by eliminating TCP packets.

22. **Claims 23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Levosky (US 2002/0087641) in view of Iptables.

Regarding **claims 23-24**, Levosky discloses all of the limitations as described above except for closing a connection using the network layer, or an IP layer, without sending messages back over the data link. In applicant's specification on page 10, lines 13-19, this can be accomplished with modification of a firewall code as to block TCP messages. The general concept of using a firewall to block certain TCP messages is well known in the art as illustrated by Iptables. Iptables is a firewall for computers in which the codes can be simply defined in tables of rules. The options can delete the packets as described in page 2, specify what protocol to watch for as described in page 3, and specify what TCP extensions to watch for in page 5. Using this firewall setup, a server could effectively block outgoing TCP FIN messages, therefore creating, according to the applicant, a silent network layer or IP layer connection drop. It would have been obvious to one of ordinary skill in the art at the time of invention to modify Levosky with using firewall codes as taught by Iptables in order to make use of the firewall's features and change them to silently close the connections as to reduce network congestion by eliminating TCP packets.

23. **Claims 27-28** are rejected under 35 U.S.C. 103(a) as being unpatentable over MacIntosh et al. (US 6,973,481) in view of Hasegawa (US 2006/0031298).

Regarding **claims 27-28**, MacIntosh et al. discloses all of the limitations as described above except for downloading a file identified within the message and downloading an image file identified by an image reference within the message. The

general concept of accessing files referenced by spam mail is well known in the art as illustrated by Hasegawa. Hasegawa teaches a spam mail filtering system that access web pages identified by URL's included in the mail message or even including in redirect tags in order to correctly filter out spam mail (section 0039 and 0058, where URL's are extracted and compared or downloaded to check for redirect code). Hasegawa specifically teaches about URL's to include web sites, however a definition of a URL as provided by SearchNetworking.com Definitions reads that a URL can access any file, including image files. It would have been obvious to one of ordinary skill in the art at the time of invention to modify MacIntosh et al. with accessing and downloading URL's identified by mail messages in order to completely filter out spam that tries to fool domain only filters as noted in Hasegawa's disclosure in sections 0005-0006.

24. **Claims 30 and 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over MacIntosh et al. (US 6,973,481) in view of "Understanding Your Quota".

Regarding **claims 30 and 39**, MacIntosh et al. discloses all of the limitations as described above except for allowing an address to be valid again after the number of messages falls below a second predetermined number within a second predetermined time. The general concept of making a email address valid again after the number of messages falls within a certain time period is well known in the art as illustrated by "Understanding Your Quotas". "Understanding Your Quotas" teaches that mail quotas are used to limit the amount of information one can store on a server, and that once a user passes a soft quota, the user has seven days to make more space in the folder or the user will not have full write privileges and can no longer accept any new files, and

this is seen as invalidating a user's address (page 2). The user will be valid again, seen as being able to perform operations on the system, if the number of mail messages falls below the soft quota in the time allotted. It would have been obvious to one of ordinary skill in the art at the time of invention to modify MacIntosh et al. with using soft quota limits to validate users as taught by "Understanding Your Quota" in order to make sure the user has a fair share of resources as noted in "Understanding Your Quota" on page 1.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Adam S. Weintrop whose telephone number is 571-270-1604. The examiner can normally be reached on Monday through Friday 7:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-6681. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AW 4/19/07

FRANTZ JULES
SUPERVISORY PATENT EXAMINER